FIG. 1A

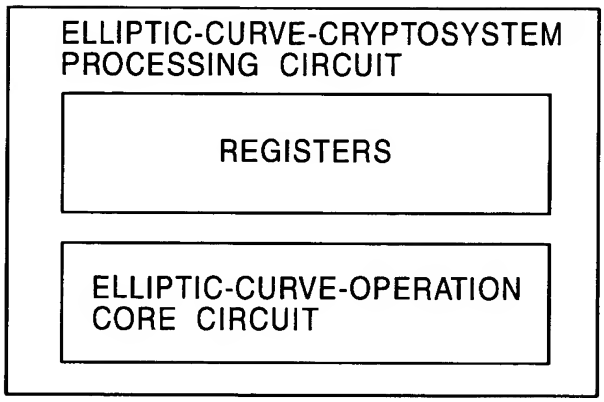


FIG. 1B

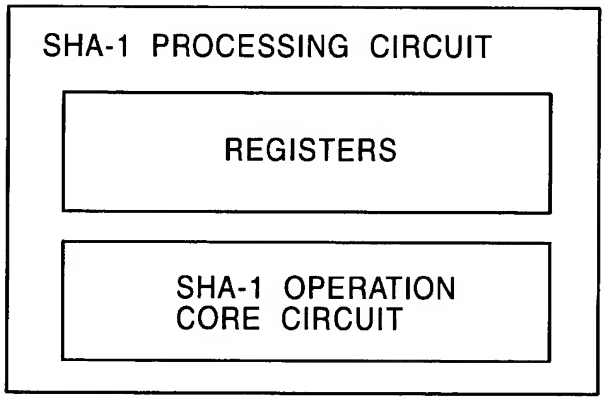


FIG. 1C

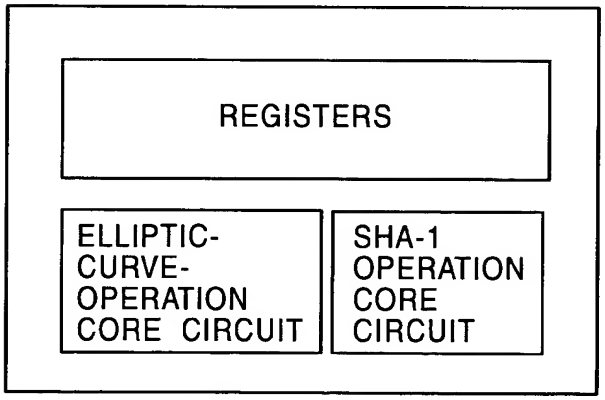


FIG. 2

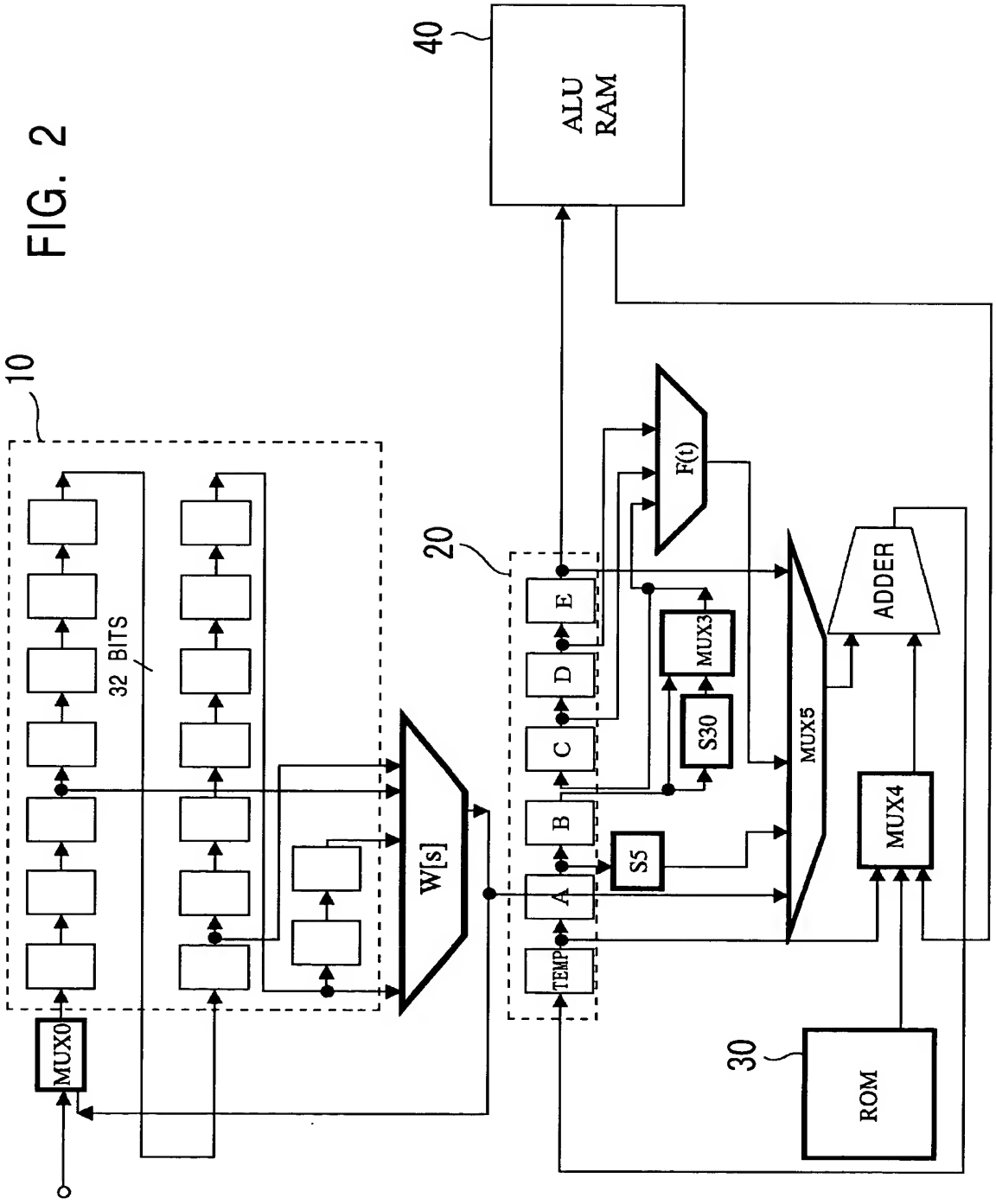

40
ALU RAM
10
32 BITS
MUX0
W[s]
20
E
D
C
B
A
TEMP
F(t)
MUX3
S30
S5
MUX5
ADDER
MUX4
30
ROM

FIG. 3

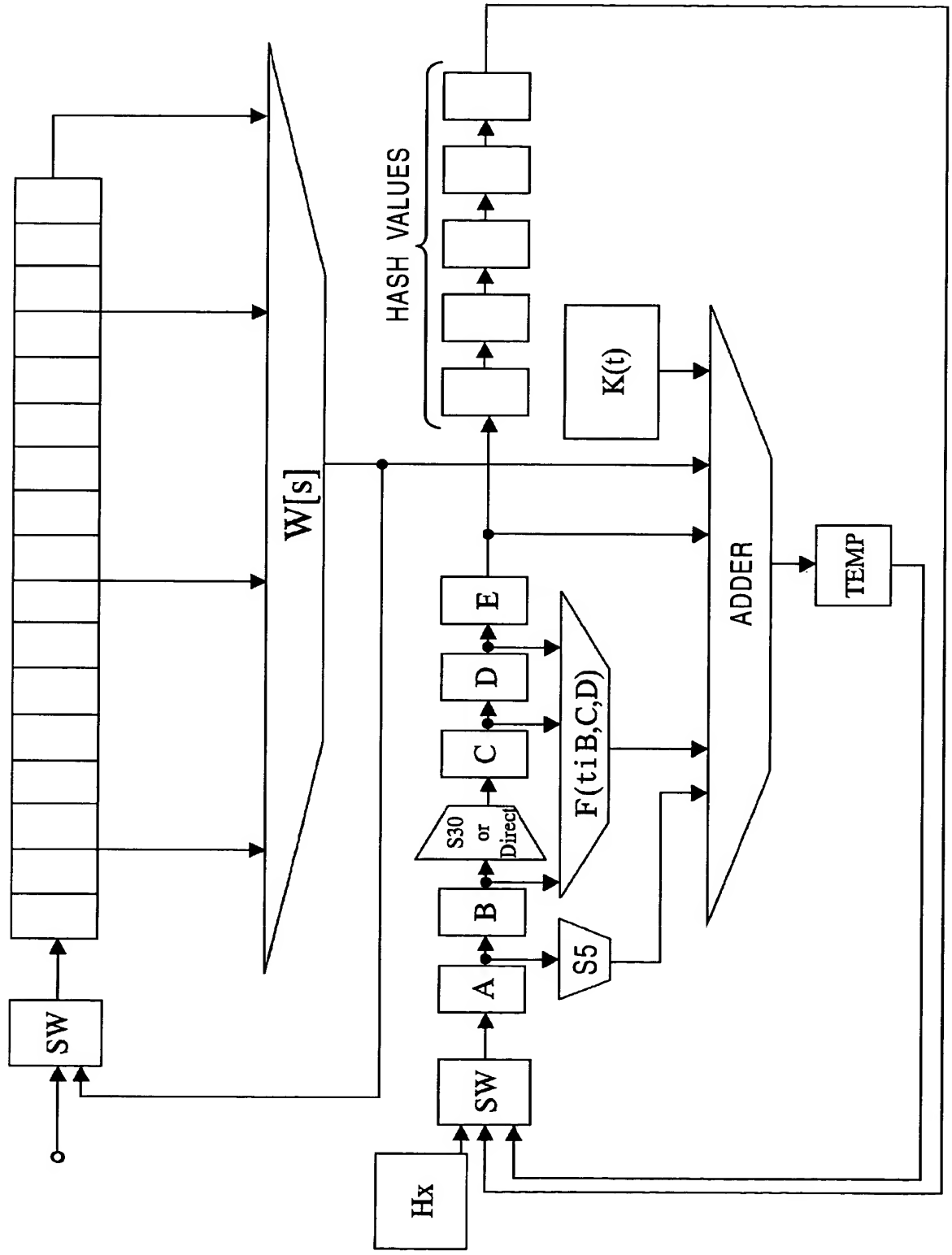

SW
W[s]
HASH VALUES
K(t)
ADDER
TEMP
E
D
C
B
A
S30 or Direct
F(tiB,C,D)
S5
SW
Hx

FIG. 4

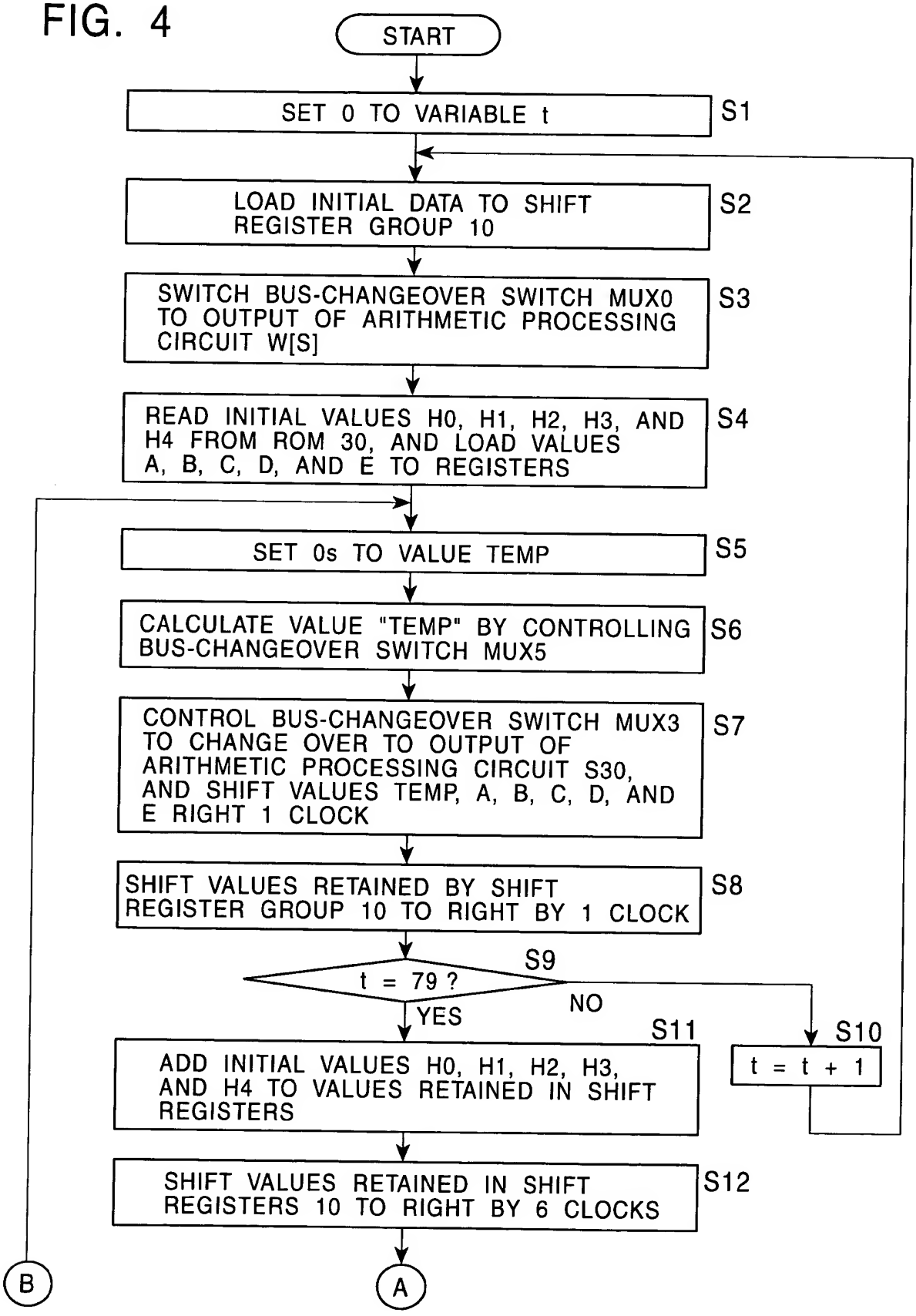

START
SET 0 TO VARIABLE t
S1
LOAD INITIAL DATA TO SHIFT REGISTER GROUP 10
S2
SWITCH BUS-CHANGEOVER SWITCH MUX0 TO OUTPUT OF ARITHMETIC PROCESSING CIRCUIT W[S]
S3
READ INITIAL VALUES H0, H1, H2, H3, AND H4 FROM ROM 30, AND LOAD VALUES A, B, C, D, AND E TO REGISTERS
S4
SET 0s TO VALUE TEMP
S5
CALCULATE VALUE "TEMP" BY CONTROLLING BUS-CHANGEOVER SWITCH MUX5
S6
CONTROL BUS-CHANGEOVER SWITCH MUX3 TO CHANGE OVER TO OUTPUT OF ARITHMETIC PROCESSING CIRCUIT S30, AND SHIFT VALUES TEMP, A, B, C, D, AND E RIGHT 1 CLOCK
S7
SHIFT VALUES RETAINED BY SHIFT REGISTER GROUP 10 TO RIGHT BY 1 CLOCK
S8
t = 79 ?
S9
YES
NO
ADD INITIAL VALUES H0, H1, H2, H3, AND H4 TO VALUES RETAINED IN SHIFT REGISTERS
S11
t = t + 1
S10
SHIFT VALUES RETAINED IN SHIFT REGISTERS 10 TO RIGHT BY 6 CLOCKS
S12
B
A

FIG. 5

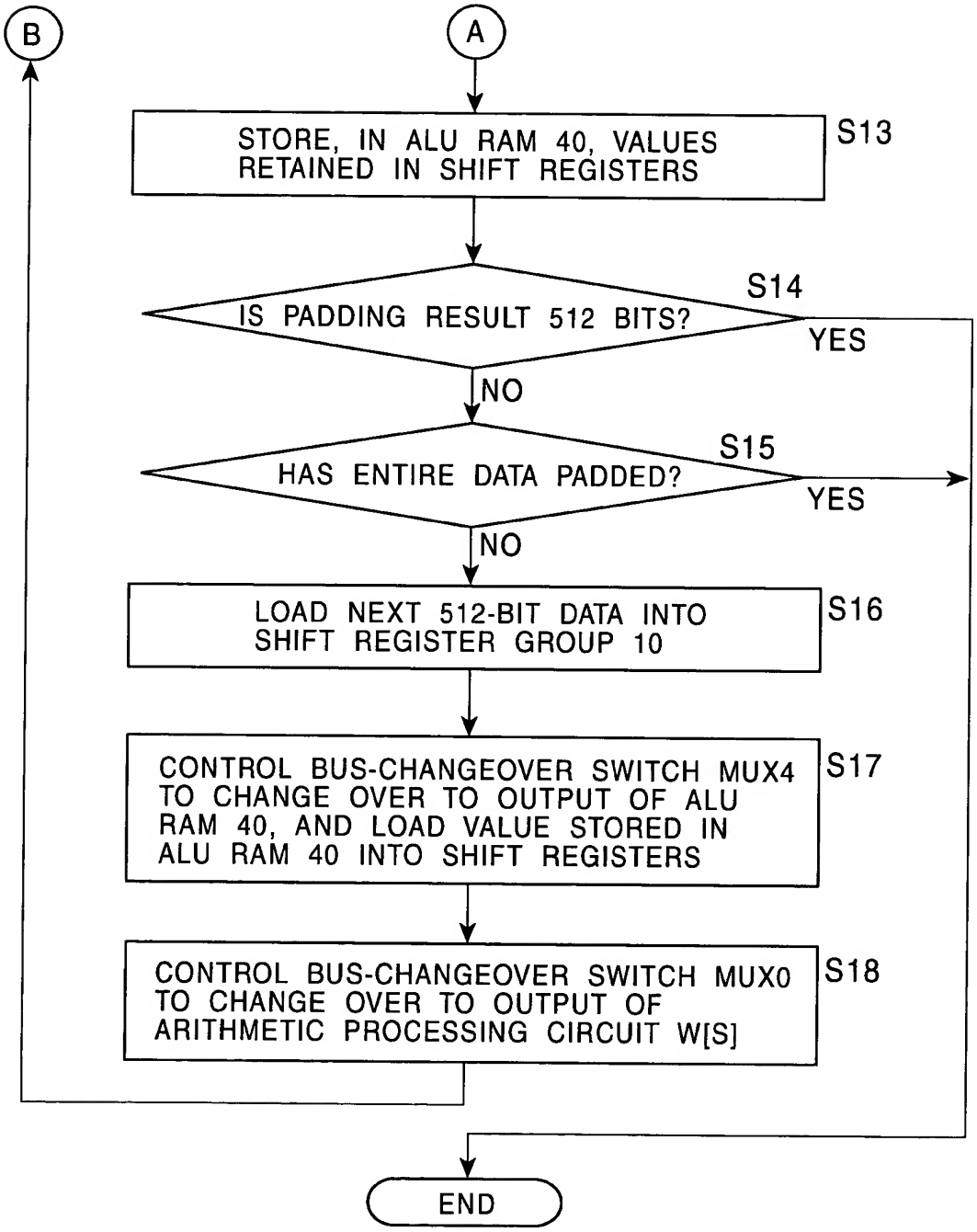
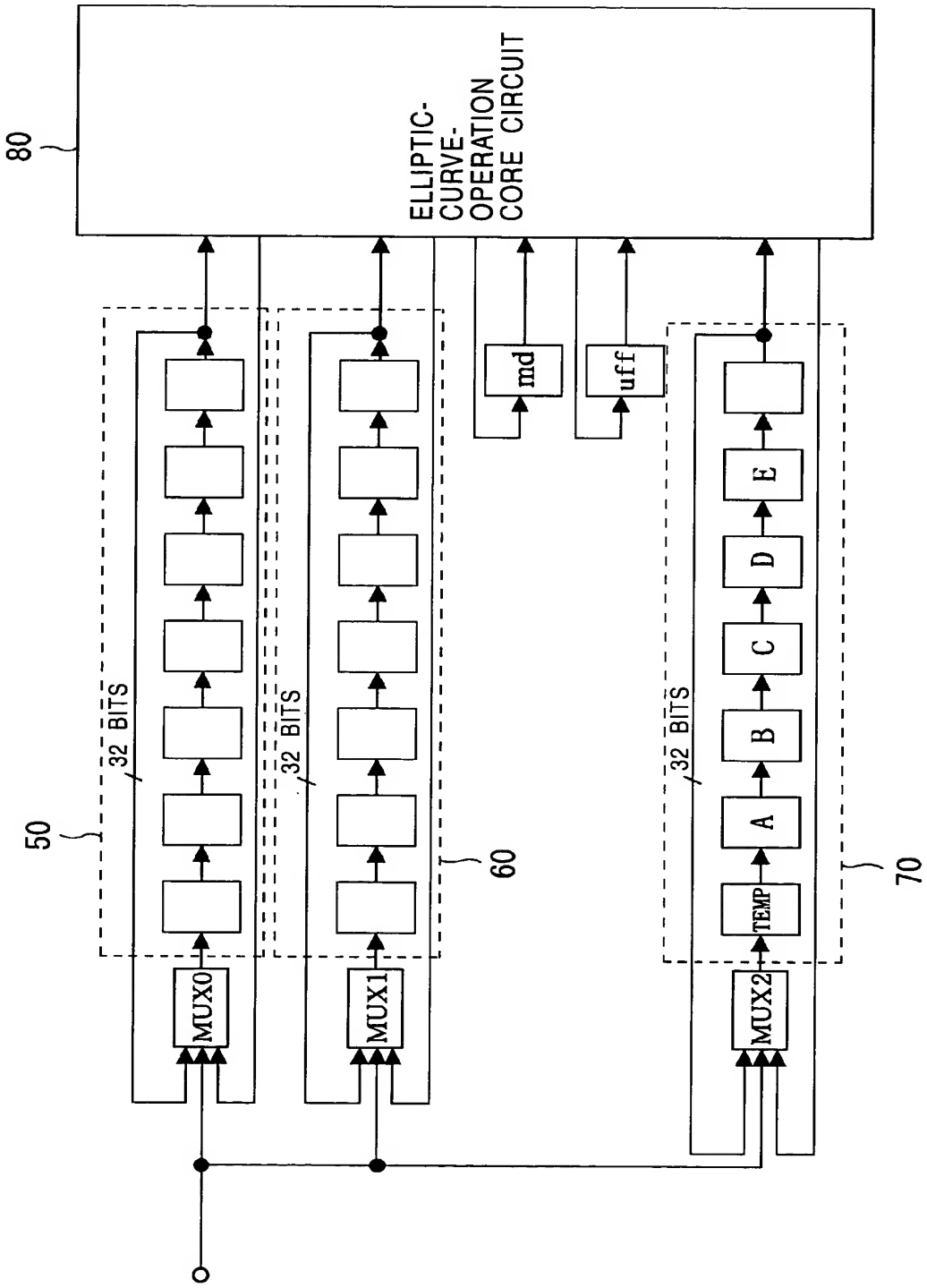

B
A
STORE, IN ALU RAM 40, VALUES RETAINED IN SHIFT REGISTERS
S13
IS PADDING RESULT 512 BITS?
S14
YES
NO
HAS ENTIRE DATA PADDED?
S15
YES
NO
LOAD NEXT 512-BIT DATA INTO SHIFT REGISTER GROUP 10
S16
CONTROL BUS-CHANGEOVER SWITCH MUX4 TO CHANGE OVER TO OUTPUT OF ALU RAM 40, AND LOAD VALUE STORED IN ALU RAM 40 INTO SHIFT REGISTERS
S17
CONTROL BUS-CHANGEOVER SWITCH MUX0 TO CHANGE OVER TO OUTPUT OF ARITHMETIC PROCESSING CIRCUIT W[S]
S18
END

FIG. 6


80
ELLIPTIC-CURVE-OPERATION CORE CIRCUIT
md
uff
50
60
70
32 BITS
32 BITS
32 BITS
MUX0
MUX1
MUX2
TEMP
A
B
C
D
E

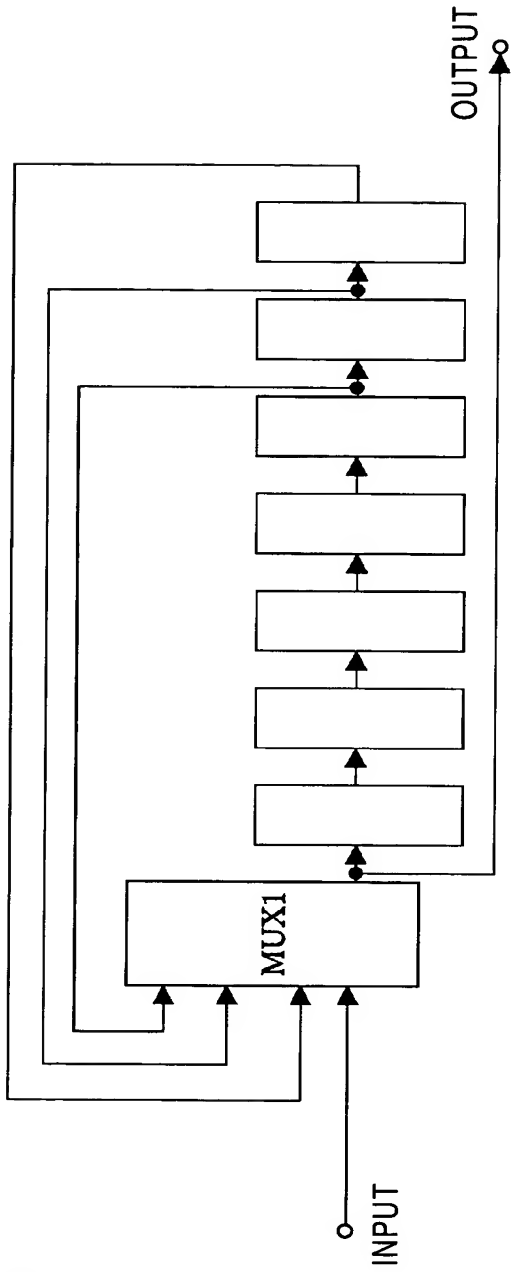


FIG. 7A

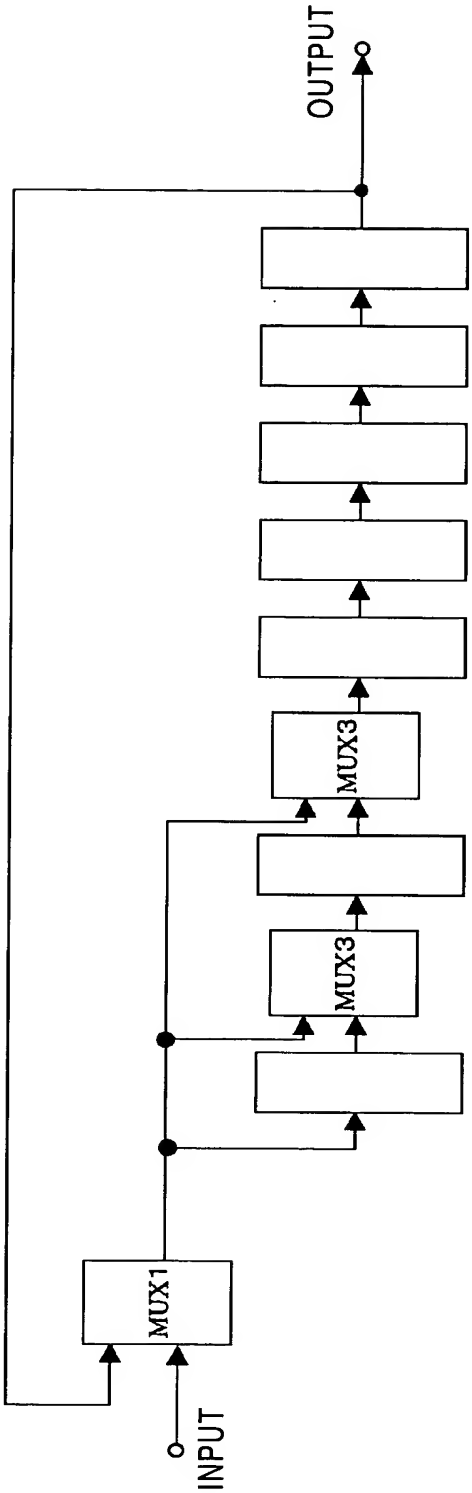


FIG. 7B

FIG. 8

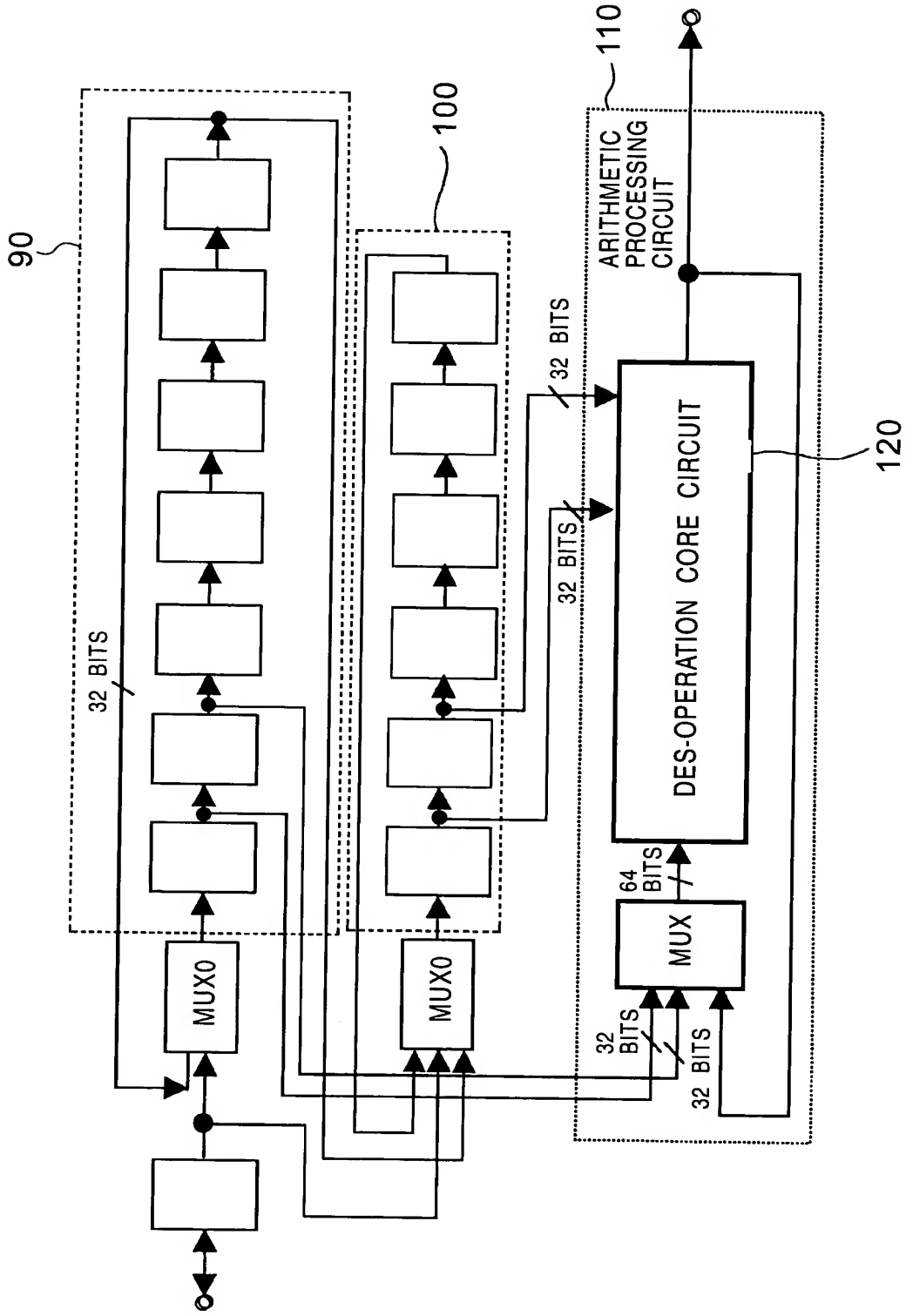

90
100
110
ARITHMETIC PROCESSING CIRCUIT
32 BITS
32 BITS
32 BITS
DES-OPERATION CORE CIRCUIT
120
64 BITS
MUX
32 BITS
32 BITS
MUX0
MUX0

FIG. 9

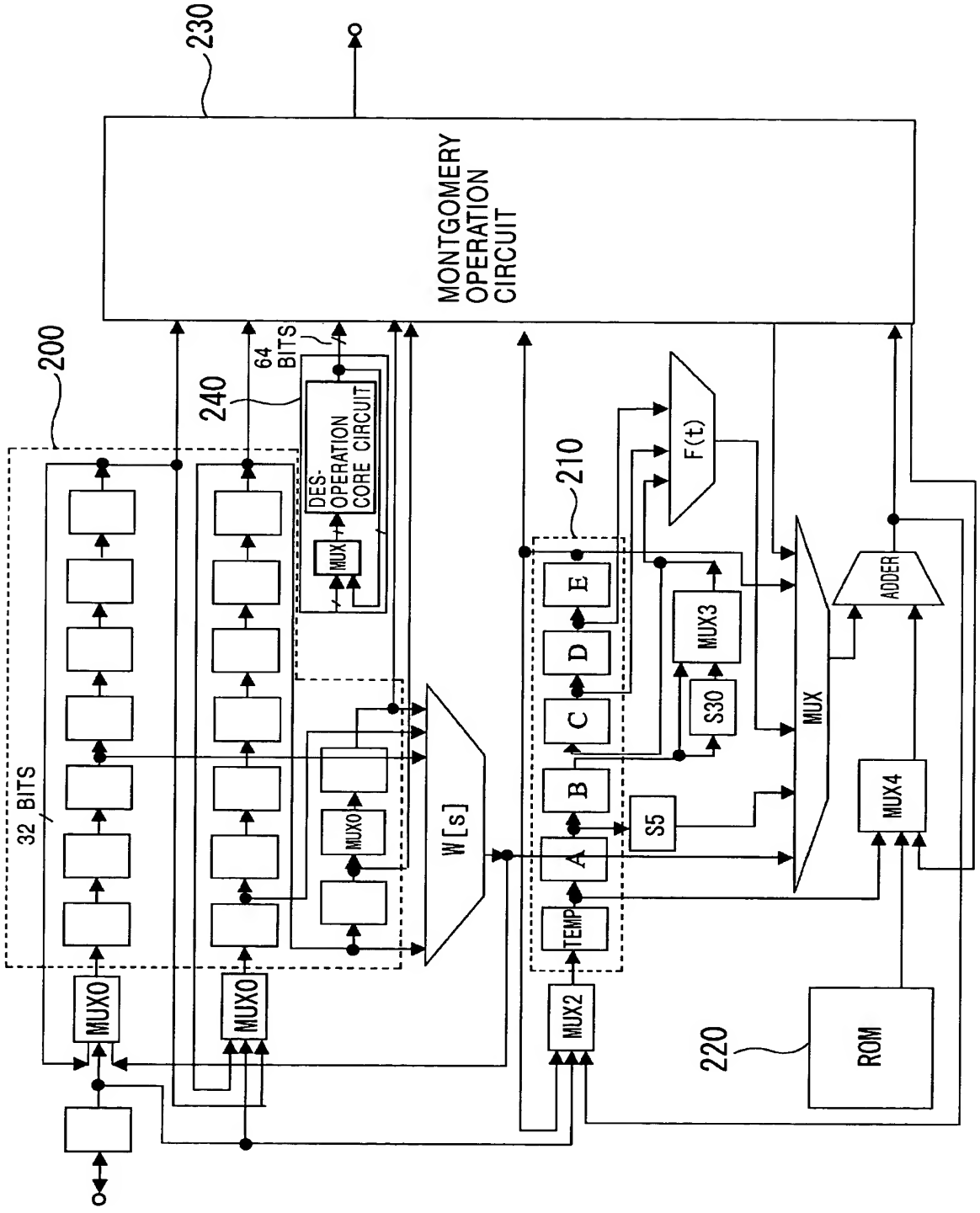

230
MONTGOMERY OPERATION CIRCUIT
200
240
64 BITS
DES-OPERATION CORE CIRCUIT
MUX1
210
F(t)
E
D
C
B
A
TEMP
MUX3
S30
MUX
ADDER
MUX4
S5
32 BITS
MUX0
MUX0
MUX0
W[s]
MUX2
220
ROM

FIG. 10

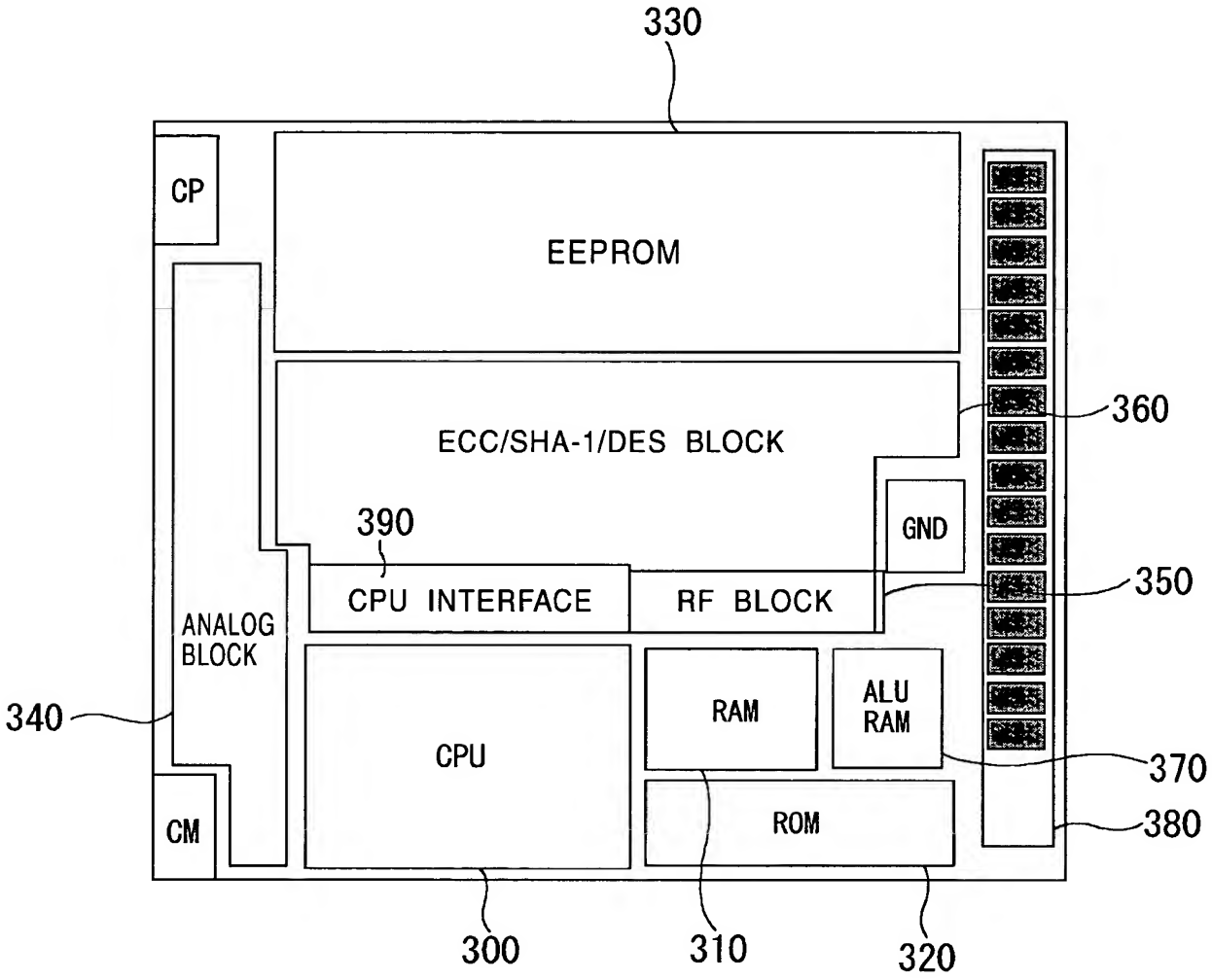

330
CP
EEPROM
ECC/SHA-1/DES BLOCK
360
390
GND
CPU INTERFACE
RF BLOCK
350
ANALOG BLOCK
340
CPU
RAM
ALU RAM
370
CM
ROM
380
300
310
320

FIG. 11

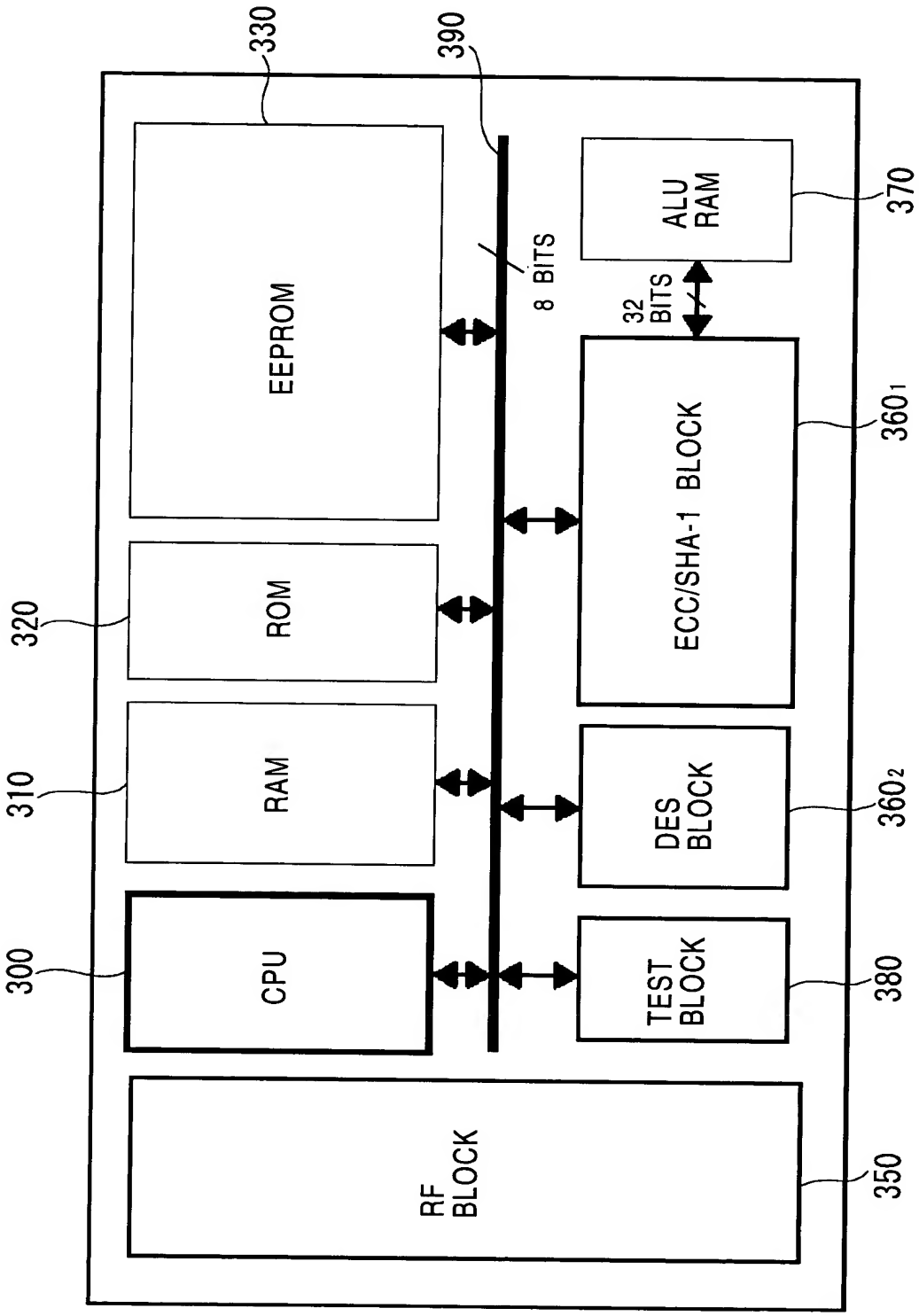

330
390
EEPROM
8 BITS
ALU RAM
370
32 BITS
320
ROM
ECC/SHA-1 BLOCK
360₁
310
RAM
DES BLOCK
360₂
300
CPU
TEST BLOCK
380
RF BLOCK
350

FIG. 12A

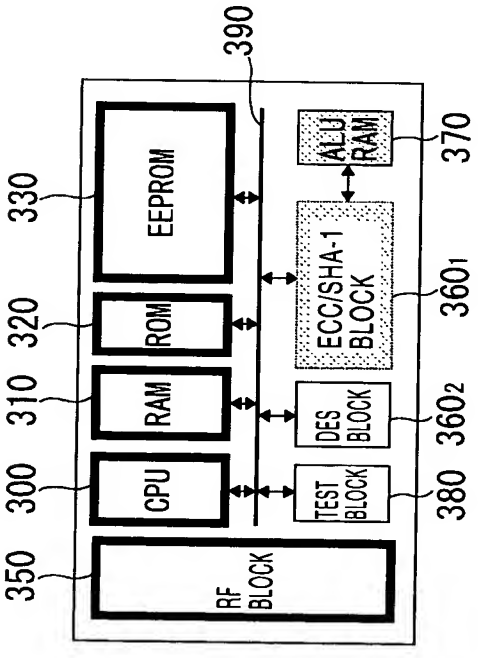


FIG. 12B

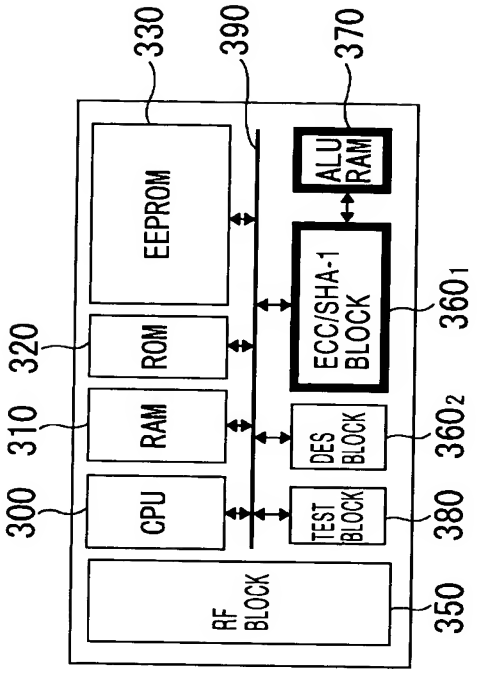


FIG. 12C

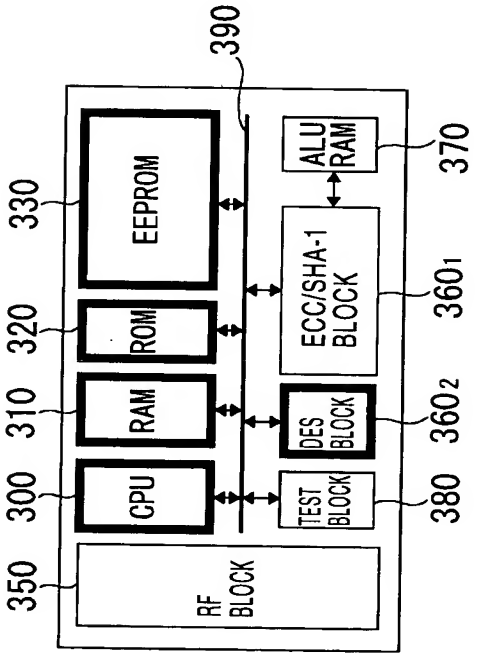


FIG. 12D